Policy
Procedure
College Standard
Standard Operating Procedure
Guideline
Local Practice

Procedure Title	Procedure Number	
Privacy Breach Management	**AD-CO-4.14a**	
Executive Responsible	Administrator Responsible	
VP Finance & Corporate Services	**Director, Policy, Planning & Strategy**	
Approving Body	Approval Date	Date of Next Review
Executive Committee	**June 3, 2026**	**June 2031**
Associated Policy and Resources		
Freedom of Information and Protection Privacy Policy and Procedure		

PURPOSE

To outline the steps for reporting, containing, assessing, and managing privacy incidents and privacy breaches to ensure timely response, mitigate risk of harm, and comply with the *B.C. Freedom of Information and Protection of Privacy Act (FIPPA)*. This procedure applies to all College of New Caledonia (CNC) employees and governs the reporting, containment, assessment, notification, and resolution of privacy incidents and privacy breaches involving personal information.

PROCEDURE

1. CNC's Approach to Managing Privacy Incidents and Breaches

1.1 The College of New Caledonia manages privacy incidents and privacy breaches in a manner that is timely, confidential, proportionate, transparent, and focused on harm reduction and prevention.

1.2 CNC is committed to:

a) Responding promptly to all reported privacy incidents to contain risk and prevent further unauthorized access, use, or disclosure of personal information.

b) Assessing privacy breaches based on the nature, sensitivity, and volume of the personal information involved and the potential for harm to individuals and the College community.

c) Taking a proportionate and risk-based approach to mitigation, notification, and corrective actions, consistent with FIPPA requirements and guidance from the Office of the Information and Privacy Commissioner of British Columbia (OIPC).

d) Communicating transparently with affected individuals and oversight bodies when notification thresholds are met.

e) Using privacy incidents and breaches as opportunities to strengthen safeguards,

improve practices, enhance awareness and education, and prevent recurrence.

1.3 CNC's response to privacy incidents and breaches is coordinated through the Privacy Office, which leads assessment, response, notification, education, documentation, and continuous improvement activities in collaboration with relevant internal departments.

1.4 Where appropriate, CNC may seek external legal advice or specialist privacy guidance to support the assessment and management of complex, high-risk, or novel privacy incidents or breaches, including advice related to regulatory compliance, notification obligations, or risk mitigation.

2. Reporting and Containment

2.1 Any employee who becomes aware of, or suspects, a privacy incident must immediately report the incident to:

a) the Privacy Office at 250-561-5888 or foipp@cnc.bc.ca, and
b) their direct supervisor.

2.2 Where a privacy incident involves a lost or stolen device or technological or system-related issue, the employee must also report the incident to IT Services by emailing helpdesk@cnc.bc.ca.

2.3 Employees must not alter, delete, destroy, or further disclose records related to the privacy incident unless directed to do so by the Privacy Office.

2.4 The Privacy Office will provide direction and guidance to employees on the appropriate steps to respond to the privacy incident.

2.5 Employees must follow all instructions provided by the Privacy Office and, where applicable, IT Services, to contain the privacy incident by taking immediate steps to prevent further unauthorized access, use, or disclosure of personal information.

a) The Privacy Office and IT Services may notify additional individuals or areas as necessary to support effective containment.
b) The Privacy Office will collect and document relevant information to determine whether a privacy breach has occurred.

2.6 Where the Privacy Office determines that a privacy breach has not occurred, the Privacy Office will notify the employee and their supervisor and may provide recommendations to reduce the risk of future privacy incidents.

3. Assessing and Mitigating Risk

3.1 Where a privacy breach has occurred, the Privacy Office will assess the nature and severity of the breach, including the potential risks and harms to affected individuals and to the College.

a) The Privacy Office may consult with relevant College employees or departments to ensure an accurate assessment of risk.
b) Where appropriate, the Privacy Office will inform relevant employees of the identified risks and potential harms.

3.2 Where a privacy breach presents an imminent risk of harm to individuals or to

the College community, the Privacy Office will notify and coordinate with the Director of Safety and Security.

3.3 Where a privacy breach involves a cybersecurity risk, the Privacy Office will notify and coordinate with the Chief Information Officer.

3.4 The Privacy Office will collaborate with relevant areas, including IT Services, Safety and Security, risk management, and the applicable department supervisor, to:

a) Identify and implement measures to mitigate the risk of harm to affected individuals and the College community; and
b) Identify and recommend corrective actions to prevent similar privacy breaches from occurring in the future.

4. Escalation of Privacy Breaches

4.1 Where a privacy breach presents heightened risk to the College, the Privacy Office will escalate the matter to the Vice President, Finance and Corporate Services. Factors that may warrant escalation include, but are not limited to:

a) Potential for significant harm to affected individuals;
b) Potential for reputational harm to the College;
c) Involvement of a large number of individuals or particularly sensitive personal information;
d) Legal, regulatory, or financial risk to the College; or
e) Anticipated media, public, or external stakeholder attention.

4.2 Escalation may occur at any stage of the breach response process and does not replace notification obligations under FIPPA.

5. Notifications

5.1 Where the Privacy Office determines that a privacy breach could reasonably be expected to result in significant harm, as defined under FIPPA, the Privacy Office will:

a) Notify the Office of the Information and Privacy Commissioner of British Columbia (OIPC); and
b) Notify affected individuals in a manner that is appropriate to the circumstances of the breach and compliant with FIPPA requirements.

6. Records and Reporting

6.1 Records related to privacy incidents and breaches will be maintained by the Privacy Office in accordance with CNC's records retention requirements and applicable legislation.

6.2 The Privacy Office will report confirmed privacy breaches to the Vice President, Finance and Corporate Services.

6.3 Aggregated or de-identified information related to privacy incidents and breaches may be used by the Privacy Office to support risk management, reporting, training, and continuous improvement initiatives.

ROLES AND RESPONSIBILITIES

7. All CNC Employees

7.1 Complying with CNC's *Freedom of Information and Protection of Privacy Policy* by maintaining confidentiality, using secure practices, and preventing unauthorized access to or disclosure of personal information.

7.2 Completing the Freedom of Information and Protection of Privacy training in the Employee Learning Hub.

7.3 Completing the Cyber Awareness training in the Employee Learning Hub.

7.4 Identifying and alerting their supervisor to processes, tools, or practices that may increase the risk of a privacy breach.

7.5 Immediately reporting all suspected or confirmed privacy incidents to their supervisor (or designate) and to the Privacy Office.

7.6 Following all instructions provided by the Privacy Office to respond to privacy incidents and prevent future incidents or breaches.

8. Supervisors

8.1 Ensuring employees complete assigned privacy and cyber awareness training.

8.2 Supporting employees in maintaining confidentiality, using secure practices, and preventing unauthorized access to or disclosure of personal information.

8.3 Ensuring privacy incidents are reported to the Privacy Office without delay and that Privacy Office instructions are followed.

8.4 Collaborating with the Privacy Office to improve processes, systems, and practices to prevent future privacy breaches, and informing the Privacy Office of any technological, organizational, or process changes that may impact identified mitigation measures.

Definitions and Acronyms	
Access	Refers to the process for viewing or using records in the custody or control of CNC under the Act.
Act or "FIPPA"	The *BC Freedom of Information and Protection of Privacy Act*, including regulations.
OIPC	Office of the Information and Privacy Commissioner of British Columbia
Privacy Office	The area within the College that is tasked with the administration of the Act.
Personal Information	Recorded information about an identifiable individual other than business contact information, as defined in the Act.
Privacy Breach	Means a confirmed case of unauthorized access, collection, storage, retention, disposition, use, disclosure, or theft of personal information to which the Act applies.

Privacy Incident	Means a possible or pending privacy breach.
Record	Any information recorded or stored by any means whether in hard copy or electronic format. This includes, but is not limited to documents, text messages, letters, emails, telephone records, written notes, maps, drawings, photographs, video, and papers.
Unauthorized Disclosure	The disclosure, production, or provision of access to personal information to which FIPPA applies, if that disclosure, production, or access is not authorized under FIPPA.
Supporting Information	
Related Policies, Forms, Documents, Websites	Acceptable Use of CNC Information Technology Policy and Procedure CNC Privacy Breach Management Webpage CUPE Collective Agreement Faculty Association Collective Agreement
Acts and Regulations	BC Freedom of Information and Protection of Privacy Act (Part 3) BC Freedom of Information and Protection of Privacy Regulation